PATENT
Attorney Docket No. 06555.0001

NOTICE OF APPEAL TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:)
)
Michael MOVALLI et al.)
)
Application No.: 08/679,421) Group Art Unit: 2514
)
Filed: August 23, 1996) Examiner: M. Tremblay
)
For: METHOD AND APPARATUS FOR)
GENERATING SECURE)
ENDORSED TRANSACTIONS)

23#/
Appeal
Brief
5/23/00

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

APPEAL BRIEF

In support of the timely filed Notice of Appeal filed January 19, 2000, and pursuant to 37 C.F.R. § 1.192, Appellants present in triplicate their brief accompanied by a check in the amount of $205.00 to satisfy the fee under 37 C.F.R. § 1.17(c) and a one-month extension of time. This is an appeal to the Board of Patent Appeals and Interferences from the decision finally rejecting claims 1-23, 25-27, and 29-31. The appealed claims are set forth in the attached Appendix. If any additional fees are required or if the enclosed payment is insufficient, please charge the deficiencies to our Deposit Account No. 06-0916. If a fee is required for an extension of time under 37 C.F.R. § 1.136 and such fee is not accounted for above, Appellants petition for such an extension and request that the fee be charged to the Deposit Account No. 06-0916.

Real Party in Interest

The real party in interest is Orion Systems, an assignee of Michael Movalli et al. for the above-captioned U.S. Patent Application.

Related Appeals and Interferences

There are no other related pending appeals or interferences directly affected by or having a bearing on the decision in the pending appeal.

Status of Claims

Pending claims 1-23, 25-27, and 29-31 have been finally rejected and are the subject of this appeal. In the July 19, 1999, final Office Action, the Examiner objected to claims 3, 4, and 14 for informalities; rejected claims 1-4 and 24-27 under 35 U.S.C. § 103(a) as being unpatentable over "Use of the 'Signature Token' to Create a Negotiable Document" written by Donald W. Davies (hereinafter "Davies") in view of U.S. Patent No. 4,825,050 to Griffith et al. (hereinafter "Griffith"); and rejected claims 5-23 and 29-31 under 35 U.S.C. § 103(a) as being unpatentable over Davies in view of Griffith and further in view of U.S. Patent No. 5,689,565 to Spies (hereinafter "Spies").

Status of Amendments

Appellants filed an Amendment After Final on November 23, 1999. In a December 3,1999, Advisory Action, the Examiner refused to enter the Amendment After Final because according to the Examiner the amendments to the claims raised new issues that would require further consideration and/or search. Appellants also file herewith a Supplemental Amendment After Final in order to correct informalities noted by the Examiner in the Final Office Action of July 19, 1999 and to cancel claim 24.

Summary of Invention

Claim 1 is directed to a method for generating secure endorsed transactions 320 (page 1, lines 4-5). A secure endorsed transaction is produced in accordance with the claimed invention by receiving and combining data representative of a transaction 210 with a unique human identifier 220 representative of the human that endorsed the transaction (page 11, lines 19-24). Data representative of a transaction 210 includes, for example, the date, time, a merchant identification, sale items, prices and taxes (page 11, lines 20-21). The unique human identifier 220 may be, for example, a digitized signature, biometric, retinal pattern, or finger print (page 11, lines 23-24). These identifiers are defined as being associated with an individual, are unique to that individual, and are non-transferable (page 14, lines 18-21).

A processor 230 operates on the transaction data 210 and the unique human identifier 220 to generate a unique code 240 based on the transaction data 210 and the unique human identifier 220 (page 16, lines 13-15). The unique code 240 is defined such that it would be computationally infeasible to duplicate the code and it would be computationally infeasible for the processor to produce the same code from different combinations of transaction data and unique human identifier (page 16, line 22, through page 17, line 3). The process used to create the unique code may be message digest software or checksum software (page 17, lines 4-9). The unique code 240 is a secure endorsement of the transaction (page 17, lines 12-17).

Claim 2 depends from claim 1 and is directed to a step of formatting to produce a secure endorsed transaction 320. In order to create the secure endorsed transaction 320 using the unique code 240, the unique code 240 is formatted together with the transaction data 210 and the unique human identifier 220 (page 17, lines 17-24). The secure endorsed transaction 320, therefore, is comprised of the unique code 240 and the data elements used to generate the unique code (page 17, lines 17-24). The resulting combination 320 is a single representation called a single whole representation of the secure endorsed transaction. The security of the secure endorsed transaction is provided, in part, by the fact that the secure endorsed transaction incorporates all of the information necessary to verify the transaction (page 21, line 18, through page 22, line 9).

Claims 3 and 4 depend from claims 1 and 2 respectively and require a memory means. Claim 3 requires the storage in the memory means of the unique code 240, the transaction data 210, and the unique human identifiers 220. Claim 4 requires that the single whole representation is stored in the memory means. The specification teaches the use of memory storage media including a hard disk 160, a floppy disk 170, a CD-ROM or other write once readable memory (WORM), or on a smart card (page 18, lines 3-8).

Claim 5 is directed to a process for generating secure endorsed transactions in a network. The network is defined as comprising remotely distributed point of sale (POS) equipment having transaction input devices and identifier input devices (page 18, lines

23-26). The first step in the process is the reception of transaction input 210 and unique human identifiers 220 (page 18, lines 23-26). Unique codes 240 are then generated from the transaction input 210 and unique human identifiers 220 (page 18, line 26, though page 19, line 1). A unique code is defined as a secure endorsement of the transaction by the individuals corresponding to the unique human identifiers. Finally, secure endorsed transactions 320 comprising the unique codes 240, the transaction input 210, and the unique human identifiers 220, are transmitted to the central controller (page 19, lines 2-16).

Claim 6 depends from claim 5 and requires that the central controller is connectable by a telecommunications network to the POS equipment, and that the transmitting step includes a step of linking the POS equipment to the telecommunications network (page 15, lines 1-20).

Claim 7 depends from claim 6 and requires the central controller receives a signal indicating that the POS equipment has linked to the telecommunications network and further defines the linking substep as including the sending of the unique codes 240, transaction input 210, and unique human identifiers 220 to the central controller over the telecommunications network (page 15, lines 1-20).

Claim 8 depends from claim 5 and defines the transmitting step as including a substep of producing a single whole representation of the secure endorsed transaction by formatting the unique codes 240, transaction input 210, and unique human identifiers 220 (page 19, lines 1-4).

Claim 9 depends from claim 8 and recites the same limitations as claim 6 discussed above.

Claim 10 depends from claim 9 and requires that the single whole representation of the secure endorsed transactions 320 are sent over the telecommunications network to the central controller.

Claim 11 is directed to a method of generating forge-resistant, tamper resistant secure endorsed transactions (page 25, lines 1-3). The preamble to the claim defines two parties. The first party endorses the transaction and has corresponding unique human identifiers 220 (page 25, lines 11-12). The second party also endorses the transaction and has public keys 510 and related private keys 530, wherein the private keys 530 are kept secret by the second party (page 25, lines 13-24). The second party may be, for example, the merchant associated with the transaction (page 25, lines 12-13). Public and private keys are defined such that each key can decrypt data encrypted by the other key, however, it is impossible to determine the value of one key from the value of the other (page 25, lines 13-17). Further, once encrypted by one of the keys, data cannot be decrypted using that same key (page 25, lines 17-18).

The first step in the claimed method is the reception of transaction data 210, a unique human identifier 220 and a public key 510 (page 25, line 25, through page 26, line 3). The received data are used to generate a unique code 520 that is a secure endorsement of the transaction (page 26, lines 3-10). The unique code 520 is defined as being unique to the particular inputs used to generate it, computationally infeasible to duplicate, computationally infeasible to produce from different inputs, and verifiable as being derived from the input data (page 26, lines 5-10).

The final step in the method is the generation of a digital signature of the unique code using the private key of the second party (page 25, lines 11-14). The digital signature 550 is defined as a secure endorsement of the transaction by the second party (page 26, lines 14-17).

Claim 12 depends from claim 11 and requires the formatting of the digital signature 550, the transaction data 210, unique human identifier 220, and public key 510 to produce a single whole representation of the tamper resistant secure endorsed transaction (page 27, lines 15-19).

Claims 13 and 14 depend from claims 11 and 12 respectively and require a memory means. Claim 13 requires the storage of the digital signature 550, the transaction data 210, the unique human identifier 220, and pubic key 510 in the memory means. Claim 14 requires the storage of the single whole representations of the tamper resistant secure endorsed transaction in the memory means. The disclosed memory means are discussed above with respect to claim 3.

Claim 15 is directed to a method of verifying secure endorsed transactions 320. The secure endorsed transaction 320 is comprised of transaction data 210, unique human identifiers 220, and unique codes 240 generated from the transaction data 210 and the unique human identifiers 220 (page 21, lines 18-24). The first step in the method is the reception of the secure endorsed transactions 320 (page 21, lines 8-13). The transaction data 210 and unique human identifier 220 of the secure endorsed transaction 320 are then processed to produce unique codes 410 (page 21, line 24, through page 22, line 1). The final step in the method is the comparison of the unique codes 410 against the unique codes 240 (page 22, lines 1-4). If a match occurs from the comparison step no alterations of the transaction data 210 or unique human identifiers 220 occurred before the verification process (page 22, lines 4-9).

Claim 16 is directed to a process for verifying secure endorsed transactions 320 on a network. The network comprises a central controller and remotely distributed POS equipment (page 18, line 23, through page 19, line 5). POS equipment includes a transaction input device and an identifier input device (page 18, lines 23-25). The first step in the method is the reception of secure endorsed transactions 320 (page 21, lines 8-13). Using the transaction data 210 and unique identifiers 220 of the secure endorsed transaction unique codes 410 are generated (page 21, line 24, through page 25, line 1). The unique codes 410 are secure endorsements of the transaction data 210 by the parties corresponding to the unique identifiers 220. The unique codes 240 are then compared against the unique codes 410 to determine if they match (page 22, lines 1-9). Based on the relationship between the data 210 and 220 used to generate the unique codes 240 and the unique codes 240, it can be determined whether the data 210 and 220 used to generate the code 240 was changed before the verification process (page 22, lines 1-22).

Claim 17 depends from claim 16 and requires that the comparison step including a substep of transmitting verification signals to the central controller indicating that neither the transaction data nor the unique identifiers of the secure endorsed transaction have been altered (page 22, lines 14-22).

Claim 18 depends from claim 16 and requires that the POS equipment includes an output display. The step of comparing of claim 16 is defined as including a substep of displaying verification messages indicating that neither the transaction data 210 nor unique identifiers 220 of the secure endorsed transaction 320 have been altered (page 22, lines 14-22).

Claim 19 is directed to a method of verifying a tamper-resistant secure endorsed transaction. The secure endorsed transaction comprises transaction data 210, a unique identifier 220 corresponding to a first party, a public key 510 corresponding to a second party, and a digital signature 550 generated using a private key 530 corresponding to the public key 510. The unique identifier 220 endorses the transaction on behalf of the first party and the digital signature 550 endorses the transaction on behalf of the second party.

After the tamper resistant secure endorsed transaction 620 is received, the digital signature and the public key are used to generate a stored unique code 710 (page 31, lines 7-14). Next, the public key 510, the human identifier 220, and transaction data 210 are used to generate a unique code 720 (page 31, lines 11-14). The final step in the method is the comparison of the unique code 720 with the stored unique code 710 (page 31, lines 17-21). A match confirms that the transaction data 210 and human identifier 220 have not been altered (page 31, line 23, through page 32, line 3).

Claims 20, 25, and 29 depend from claims 5, 1, and 11 respectively, and define the POS equipment as including a smart card device 130 for reading/writing card data from the smart card (page 14, lines 22-26). The receiving step of claim 5 includes the substep of receiving signals from the smart card device indicating the insertion of smart cards and acquiring card data from the inserted smart cards for inclusion in the transaction data (page 18, lines 8-10).

Claims 21, 26, and 30 depend from claims 20, 25, and 29 respectively, and define the transmitting step as including dispatching the secure endorsed transactions to the inserted smart cards (page 18, lines 6-8).

Claims 22, 27, and 31 depend from claims 20, 26, and 30 respectively and define the transmitting step as including writing the secure endorsed transactions on the inserted smart cards (page 18, lines 6-8).

Claim 23 is directed to a process for generating secure endorsed transactions on a network. The network is comprised of a central controller and remotely distributed POS equipment. The POS equipment includes a transaction input device for transaction input and an identifier input device for unique identifiers (page 14, lines 11-21). The POS equipment is optionally connected to a smart card device for reading/writing card data from smart cards and writing data representative of secure endorsed transactions to smart cards (page 18, lines 6-19).

The process includes the reception of a signal indicating the insertion of a smart card in the smart card device. Next card data is read from the inserted smart card (page 18, lines 8-12), and transaction input is received from the transaction input device (page 16, lines 5-10). The card data and transaction input are combined to form transaction data 210 representative of the transaction (page 8, lines 24-26). A human identifier 220 corresponding to the party endorsing the transaction is received from the identifier input device (page 14, lines 11-21). A unique code 240 constituting an endorsement of the transaction is generated from the transaction data and the unique identifier (page 16, lines 22-26). Finally the unique code 240, transaction data 210, and unique identifier 220 are stored on the smart card (page 18, lines 6-8) as a secure endorsed transaction.

Issues

The issues presented in this appeal brief are:

A. Whether claims 1-4 and 25-27 were properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Davies in view of Griffith.

B. Whether claims 5-23 and 29-31 were properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Davies in view of Griffith and further in view of Spies.

Grouping of Claims

The following groups of claims are considered to be separately patentable:

Group I: Claims 1, 3, and 25-27

Group II: Claims 2 and 4

Group III: Claims 5-7 and 20-22

Group IV: Claims 8, 9 and 10

Group V: Claim 11-14 and 29-31

Group VI: Claim 15-18

Group VII: Claim 19

Group VIII: Claim 23

The groups of claims do not stand or fall together. The reason Appellants consider the groups of claims to be separately patentable is that the groups of claims define different embodiments of the present invention and define these embodiments in varying levels of detail.

Argument

A. Claims 1-4 and 25-27 have been improperly rejected under 35 U.S.C. § 103(a) as being unpatentable over Davies in view of Griffith.

1. Group I: Claims 1, 3, and 25-27

Regarding claim 1, Appellants respectfully assert that these claims were improperly rejected based on the combination of Davies and Griffith.

The portion of the Davies reference cited by the Examiner refers to the use of a signature token for use in performing transactions (page 378). The signature token is a "smart card" with its own display and key-pad, which can generate a digital signature (page 378).

Davies does not expressly explain the process of generating a digital signature. According to *Digital Signature Guidelines Tutorial,* A.B.A. Sec. Sci. and Tech. Info. Security Comm., digital signatures consists of the results of the operation of an encryption algorithm using two different but mathematically related keys, one public, which is publicly available, and one private, which is known only to the signer. The application of the algorithm to the data using one key transforms the data into encrypted form and the application of the algorithm using the other returns the data to its original form. The creation of a digital signature also includes a process called a "hash function," which is used in creating and verifying the signature. The hash function operates on the data to be signed to create a hash value of standard length that is substantially unique to the data.

The basic operation of creating and authenticating a digital signature is to feed the message to be signed into the hash function to create a hash value. The hash value is then encrypted using the signer's private key. In order to verify the authenticity of the message, the signer's public key is used to decrypt the message to its original hash value form. The message itself is then operated on by the hash function to create a new hash value which can be compared to the generated hash value in order to verify that the message has not been changed.

Returning to the Davies reference, the Examiner asserts that Davies teaches:

> receiving transaction data (9, 10, 11, 12, 14, and 15) corresponding to a transaction and at least one unique identifier of a customer (typically a human) (5); and generating a unique code 16 from the transaction data and the unique identifier of a customer, wherein the unique code constitutes a secure endorsement of the transaction by the party corresponding to the unique identifier.

The element of Davies cited by the Examiner as a unique human identifier is "5 customer identity." Appellants respectfully assert that it is unreasonable to interpret a customer identity as a unique human identifier. The Examiner asserts at page 4 of the Final Office Action that "customer identity must be interpreted as a unique number which reliably and uniquely identifies a single customer." The Examiner appears to assert that, as with paper checks, a number identifying the account number corresponding to the check must be used. Initially Appellants note that there is no requirement that an account number be unique to an individual, as joint bank accounts and joint credit card accounts clearly show. Further, there is no requirement that the account number on the check is in fact unique to the individual. The only requirement is that the account number, in combination with the bank's routing number identifies a particular account at a particular bank. The bank's routing number would not be a part of customer identity, and in fact, in accordance with the Examiner's interpretation of Davies would be separately signed by the central bank (see Fig. 1).

Further, Appellant clearly defined the term unique identifier in the specification at page 14, lines 18-21, such that a unique identifier is "associated with an individual . . . is unique to the individual and non-transferrable." According to M.P.E.P. § 2111.01 "Applicant may be his or her own lexicographer as long as the meaning assigned to the term is not repugnant to the term's well known usage. *In re Hill*, 161 F.2d 367, 73 USPQ 482 (CCPA 1947)." Therefore, even if the Examiner correctly interpreted customer identity 5 of Davies as an account number, such an account number not only is transferrable, but as discussed above could belong to more than one individual. In contrast, the individual identifiers of Appellant's invention, for example a retinal pattern, are not transferrable as they are characteristics of the individual, not a number assigned to the individual.

Further, the claim expressly requires that the unique code is generated from the transaction data and the unique human identifiers. Even if customer identity 5 of Davies could reasonably be interpreted as a unique human identifier as claimed, that element of Fig. 1 is not used in creating signature 16. Specifically, Fig. 1 of Davies states that signature 16 is a signature of elements 9-15, which include: check sequence no. 9; transaction type 10; amount of payment 11; currency 12; beneficiary identity 13;

description of payment 14; and date and time 15. None of the information signed by signature 16 relates in any way to the identity of a specific individual. Instead, the element cited by the Examiner as an individual human identifier, customer identity 5, is expressly disclosed as being signed by the bank. Davies, therefore, fails to teach or suggest that which the Examiner cites the reference as teaching.

At page 3 of the Final Office Action, the Examiner admits that Davies fails to teach "a 'human' identifier, e.g. a biometric, can be used to such an encryption scheme to further enhance security." The Examiner continues by arguing:

> Griffith teaches that "Multiple inputs are accepted in the following manner: The individual information record 101 which is the data to be 'locked'; the individual identifier 100 which may be some characteristic of the individual e.g. finger, voice, or retinal pattern, signature, or chemical structure or some information known only to the individual, e.g. a combination, pass word or phrase; a private key 110 which is known only to the issuing entity and which is generated by any method 109 meeting the criteria for public key crypto system . . . . " Thus Griffith teaches that the public/key method can be used with a "human identifier" to thwart fraud. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to include a "human identifier" as taught by Griffith in the system taught by Davies because this would make it more difficult for a thief to use a stolen smart card, as taught by Griffith to create the negotiable documents taught by Davies.

The Examiner fails to provide any information about where or how the "characteristic of the individual" of Griffith would be used in the system of Davies to provide the advantages claimed by the Examiner. As discussed in our previous responses, the nature of the smart card of Davies is that the card "provides a microprocessor and store in [the] plastic card which is held by the bank's customer to identify him" (page 378). The advance over the prior art that is taught by Davies is "a 'smart card' with its own display and key-pad" (page 378). A security advantage of this smart card having a key pad is "[t]he PIN is checked by the card and does not enter from a 'foreign' keypad" (page 379). It is the PIN number that identifies the individual to the card, which then confirms that the individual is who he or she claims to be. The security advantage is that the PIN number is not accessible to any device other than the card itself. The Examiner asserts that there is an advantage to substituting the "characteristic of the individual" into the smart card of Davies. There is no teaching or suggestion of how the smart card itself could capture any of the types of characteristic information disclosed by Davies, and, if equipment other than the smart card itself were necessary to capture the information then an express motivation for the system of Davies is defeated. Appellants assert that Davies expressly teaches away from using any mode of individual authentication that would require information to be input from a source external to the smart card, and that therefore, the combination suggested by the Examiner is not supported by the references.

Further, the Examiner fails to address in any way the actual use in Griffith of the individual identifier 100. As shown in Fig. 1 of Griffith, the individual identifier 100 is captured and through a reduction method 103 is transformed into an individual identifier transform 106. The individual identifier transform 106 is used as a key to encode intermediate cipher text into the media cipher text 117 (column 3, lines 4-5). The use of the individual identifier transform 106 of Griffith is as a form of symmetric-key encryption. Symmetric-key encryption is an older form of encryption separate from public-key cryptography, wherein the same key that is used to encrypt a message must be used to decrypt that message. Griffith refers to this encryption scheme in the claims as "a private key cryptosystem," however, as would be understood by a person having ordinary skill in the art, this is not a reference to a private key from a public key/private key pair, but instead is a reference to a symmetric key. As discussed by Spies at column 9, lines 44-45 "[t]he symmetric key must be known to both the sender and receiver, but otherwise kept secret." In order for the encryption scheme using the individual identifier transform 106 to be useful, the individual identifier transform 106 must, therefore, not be available to the public. If the individual identifier transform 106 is not maintained secret, any party could encrypt messages using that encryption key, and so the security resulting from the encryption step would be meaningless.

In opposition to the Examiner's assertion of the obviousness of using the individual identifier 100 of Griffith in the system of Davies, Davies expressly chose to create a system using public key encryption and not secret key encryption. The well known advantage to public key encryption, specifically in the field of digital signatures, is that the party possessing a private key known only to that party can encrypt a message. Any party can thereafter access that individual's public key and decrypt the message to confirm that the party's private key was used to encrypt the message. No other party, however, need have access to the private key. Such an encryption scheme is in stark contrast to a secret key encryption using the individual identifier 100 of Davies, wherein a party having access to the secret key in order to confirm the authenticity of a message will necessarily also have the ability to create other encrypted messages using that key.

There is simply no motivation in the prior art cited by the Examiner for using the secret key encryption scheme of Griffith in the smart card system of Davies.

Regarding claims 3 and 25-27, these claims are patentable over the applied combination of references, at least, in view of their dependence from claim 1.

2. Group II: Claims 2 and 4

Claim 2 is patentable over the applied combination, at least, in view of its dependence from claim 1. Further, claim 2 requires a step of formatting the unique code, the transaction data, and the unique human identifier to produce a single whole representation of a secure endorsed transaction. The Examiner fails to address in any way this additional limitation. The rejection of claim 2, therefore, is invalid.

With specific regard to the claim limitation, the resulting data structure from the claim step, the single whole representation, is a single data element including both the unique code created from the transaction data and the unique human identifier, and the transaction data and unique human identifier. As recited in claim 1, the unique code is an endorsement of the transaction. The recited single whole representation, therefore, includes both an endorsement of the transaction and the data elements used to create that endorsement.

The Examiner asserts at page 3 of the Final Office Action that the signature 16 of Davies "constitutes a secure endorsement of the transaction by the party corresponding to the unique identifier." Without accepting the Examiner's assertion that the signature 16 of Davies is a secure endorsement of the transaction, Appellants respectfully assert any reasonable interpretation of the invention of Davies as illustrated in Fig. 1 fails to meet the express limitations of claim 2. As discussed above with respect to digital signature technology, the creation of a digital signature is accomplished by encoding information derived from a message using a private key known only to the party creating the signature. The authenticity of that message can be determined later using a public key related to the private key. Signature 16 of Davies is created by encoding a data element derived from elements 9-15 using the customer's private key. Appellants assert that a person having ordinary skill in the art would not format together the elements used to create a digital signature, as to do so would make the customer's private key public and contravene the express goal of the digital signature system.

Similarly, in Griffith, the elements used to encode media cipher text 117 are entity private key 110 and individual identifier transform 106. As discussed above, individual identifier transform 106 is used as a secret key in a symmetric-key encryption scheme. The security of both encryption schemes requires that the private key 110 and individual identifier transform 106 be maintained secret. As with the digital signature of Davies, therefore, the elements used to generate the encrypted element would not be formatted together with the encrypted element, as to do so would defeat the purpose of the encryption.

Regarding claim 4, this claim is patentable over the applied references, at least, in view of its dependence from claim 2.

B. Claims 5-23 and 29-31 have been improperly rejected under 35 U.S.C. § 103(a) as being unpatentable over Davies in view of Griffith and further in view of Spies.

3. Group III: Claims 5-7 and 20-23

Regarding the rejection of claim 5 as being unpatentable over Davies in view of Griffith, and further in view of Spies, Appellants respectfully traverse this rejection. Claim 5 is similar to claim 1, additionally requiring that the method is performed in a network comprised of a central controller and remotely distributed point of sale (POS) equipment and that the method perform an additional step of transmitting the unique codes (which are endorsements of the transactions) along with the transaction input and unique human identifiers to the central controller.

As discussed above, the Examiner cites signature 16 of Davies as an endorsement of the transaction and elements 9-15 of Davies as transaction input. The elements used to generate signature 16 are elements 9-15 as encrypted by a private key known only to the person signing the instrument. Signature 16 is not sent to a central controller along with the private key. Yet it is the private key of the individual signing the instrument that in fact provides the authentication of the transaction, *i.e.*, the method of determining whether the signature was in fact provided by the person claiming to have signed it is to decrypt the signature using the person's public key, whereby only if the decryption with the public key returns a message that could only have been generated using the person's private key is the transaction in fact deemed authentic. Because signature 16 is not generated from transaction data and a unique human identifier and then transmitted with the transaction data and unique human identifier, Davies does not teach that which the Examiner asserts it teaches.

As discussed above with respect to claim 1, Davies fails to cure the defects in Griffith. Further, Spies, which uses both public key encryption and symmetric key encryption shares the same problems as Davies and Griffith respectively when sending a message including a code and the data used to generate that code. Appellants, therefore, respectfully assert that claim 5 is patentable over any reasonable combination of Davies, Griffith, and Spies.

Regarding claims 6, 7, and 20-22, these claims are patentable over the applied references, at least, in view of their dependence from claim 5.

Regarding claim 23, this claim is patentable over the applied references for at least essentially the same reasons expressed above with respect to claim 5.

4. Group IV: Claims 8, 9, and 10

Regarding claim 8, 9, and 10, these claim are patentable over the applied references, at least, in view of their dependence from claim 5. Further, as expressed above with respect to claim 2, the combination of Davies and Griffith fails to teach or suggest a step of formatting the unique codes, transaction data and unique human identifiers to produce a single whole representation of the secure endorsed transaction. The single whole representation incorporates both the endorsement of the transaction (the unique code) and the data used to generate the endorsement (the transaction data and the unique human identifiers). Spies fails to cure the defects in the combination of Davies and Griffith, as a person having ordinary skill in the art, in view of Spies, would not have been motivated to combine an encrypted code as disclosed by Spies together with the information used to generate that code. Appellants, therefore, request that the rejection of claims 8, 9, and 10 be withdrawn.

5. Group V: Claims 11-14 and 29-31

Regarding the rejection of claim 11, Appellants respectfully traverse this rejection. Claim 11 requires that two parties are involved in the generation of a forge-resistant, tamper-resistant secure endorsed transaction. The Examiner appears to rely on the same basis of rejection provided with respect to claim 1-10 as to claim 11, as the Examiner makes no mention of the additional limitations provided in claim 11. The rejection of claim 11 as being unpatentable over Davies in view of Griffith, and further in view of Spies is facially deficient for failing to address that claim in any meaningful way.

As to the substance of claim 11, this claim requires a first party who endorses the transaction having a unique human identifier associated therewith and a second party who endorses the transaction having a public key/private key pair associated therewith. A unique code constituting a secure endorsement of the transaction by the first party is generated from transaction data, a unique human identifier associated with the first party, and the public key associated with the second party. A digital signature of the unique code is then generated using the second party's private key.

As discussed above, the Examiner interprets signature 16 of Davies as a unique code that is a secure endorsement of the transaction by the customer. Signature 16 is a digital signature created by encrypting data 9-15 using the customer's private key. This, however, is not what Appellant has claimed. The first step of the claim requires a unique code to be generated from transaction data, a unique human identifier of a first party, and a public key of a second party. Signature 16, as discussed above is generated only from what the Examiner has interpreted as transaction data (elements 9-15) and the customer's private key. Digital signature 16, therefore, is not a unique code as claimed.

Claim 11 also requires a second step, which was not remotely addressed by the Examiner in the Final Office Action. In this step, a digital signature of the unique code is generated using *a second party's private key.* Therefore, even if digital signature 16 of Davies were a unique code as claimed, there is no step after the creation of the unique code of signing that unique code using another party's private key. As disclosed in the specification, the second party could be, for example, a merchant.

Griffith and Spies also fail to teach or suggest a step of generating a unique code from transaction data, a unique human identifier and a public key of a second party and then signing the unique code with a private key belonging to the second party. Because the cited references, alone or in any reasonable combination, fail to teach or suggest Appellants method as recited in claim 11, Appellants assert that this claim is patentable over the applied combination.

Regarding claims 12-14 and 29-31, these claims are patentable over the applied combination of references, at least, in view of their dependence from claim 11.

6. Group VI: Claims 15-18

Regarding the rejection of claim 15, Appellants respectfully traverses this rejection. Claim 15 is directed to a method of verifying a secure endorsed transaction. Secure endorsed transaction is defined as comprising transaction data, unique human identifiers, and unique codes generated from the transaction data and unique human identifiers. The Examiner fails to sufficiently address in the Final Office Action any method of verifying a transaction, presumably relying on a inference that if the method of generating a transaction is rendered obvious so is the method of verifying it. Such an interpretation, however, fails to provide a valid rejection of the claims.

As discussed above with respect to claim 1, Davies in view of Griffith fail to teach or suggest the production of a secure endorsed transaction as claimed. The Examiner cites signature 16 of Davies as teaching Appellants' claimed unique code. Signature

16, however, is not generated from transaction data and a unique human identifier, but instead is an encryption of data elements 9-15 using the customer's private key.

Further, the verification process for a digital signature such as that disclosed by Davies is to decrypt the signature using the customer's public key and to compare the resulting decrypted data against a check sum or hash function of the data used to create the signature. In a digital signature verification process, the digital signature itself is never compared against anything. The reason the digital signature cannot be compared against a newly created digital signature is that in order to create a new digital signature the private key of the customer would be needed, however, to make the private key available would defeat the purpose the encryption. In other words, even if the digital signature of Davies could properly be interpreted as a unique code as claimed by Appellants, that "unique code" is not and cannot be compared against a "generated unique code" because a party verifying the authenticity of a digital signature cannot recreate the digital signature without the customer's private key.

Because the element cited by the Examiner as the unique code is never compared against a generated version of that code, Appellants respectfully assert that the rejection of claim 15 as being unpatentable over Davies in view of Griffith and further in view of Spies was in error and must be withdrawn.

Regarding claim 16, this claim is patentable over the applied references for essentially the same reasons expressed above with respect to claim 15. Regarding claims 17 and 18, these claims are patentable over the applied references, at least, in view of their dependence from claim 16.

7. Group VII: Claim 19

Appellants traverse the rejection of claim 19. As with claim 15 discussed above, the Examiner assumes that if the Examiner's interpretation of the combination of Davies, Griffith, and Spies, renders unpatentable Appellants method of generating a secure endorsed transaction, then the verification of that transaction would also be rendered obvious. The Examiner has provided no support for this position, and therefore, the rejection of claim 19 is invalid. Further, as discussed above with respect to claim 11, the Examiner fails to address any of the additional limitations recited in claim 16, such as a public key/private key pair of a second party endorsing the transaction. Because the Examiner failed to address the additional limitations in any meaningful way, the rejection of claim 16 is invalid.

Beyond simply failing to address the express limitations of the claim, any reasonable interpretation of the cited combination fails to render Appellants claimed invention obvious. As discussed above with respect to claim 15, the verification of a digital signature as disclosed by Davies would proceed as follows: a message accompanied by a signature of that message by the party sending the message is received; the signature is then decrypted using the public key of the party sending the message; next a value based on the message is generated, for example, a check sum or hash value; finally, the generated value is compared against the decrypted signature to determine if the message was altered.

As discussed above, the Examiner interpreted signature 16 of Davies as teaching Appellants claimed unique code. By no reasonable interpretation is signature

16 of Davies generated from a public key, human identifier, and transaction data. Instead signature 16 is generated from a private key and data elements 1-15.

Further, signature 16 of Davies cannot reasonably be interpreted as both the claimed digital signature and the stored unique code generated from that digital signature. The applied combination of references fails to teach or suggest both a unique code generated from a digital signature and a unique code generated from a public key, human identifier, and transaction data, and the comparison of the two unique codes to verify the process. Appellant therefore asserts that claim 16 is patentable over the applied combination of references.

Conclusion

In order to support a rejection based on a combination of references under § 103, it is necessary not only to show that disparate elements were known in the prior art, but also that a person having ordinary skill in the art would have been motivated to combine those elements together. The Examiner has failed to explain how a person having ordinary skill in the art would use the individual identifier of Griffith in the smart card system of Davies. The simple expedient of finding a reference that notes that "some characteristic of the individual" may be used in a transaction security method does not address how or why that teaching would be used in another invention. Further, even if the Examiner were able to show that the claimed method of producing a secure endorsed transaction was obvious in view of the prior art, such a showing does not in any way foreclose the patentability of a method for verifying that transaction. Finally, with respect to the method of producing secure endorsed transactions that are endorsed by two parties, the Examiner failed to even address this embodiment of the invention.

In view of the above, Appellants respectfully request a positive determination as to the patentability of Appellants' invention as recited in claims 1-23, 25-27, and 29-31.

To the extent any further extension of time under 37 C.F.R. § 1.136 is required to obtain entry of this Appeal Brief, such extension is hereby respectfully requested. If there are any fees due under 37 C.F.R. §§ 1.16 or 1.17 which are not enclosed herewith, including any fees required for an extension of time under 37 C.F.R. § 1.136, please charge such fees to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

By: Jeffrey A. Berkowitz
Reg. No. 36,743

Dated: April 19, 2000

Finnegan, Henderson, Farabow,
Garrett & Dunner, L.L.P.
1300 I Street, N.W.
Washington, D.C. 20005
(202) 408-4000

Appendix

1. A computer-implemented method of generating secure endorsed transactions, the method comprising:

receiving transaction data corresponding to a transaction and at least one unique human identifier; and

generating a unique code from the transaction data and the unique human identifier, wherein the unique code constitutes a secure endorsement of the transaction by the party corresponding to the unique human identifier.

2. The method of claim 1, wherein the generating step includes the substep of:

formatting the unique code, the transaction data, and the unique human identifier to produce a single whole representation of a secure endorsed transaction.

3. The method of claim 1, wherein the data processing system includes a storage means, and wherein the generating step includes the substep of:

storing the unique code, the transaction data, and the unique human identifier in the memory means.

4. The method of claim 2, wherein the data processing system includes a storage means, and wherein the formatting step includes the substep of:

storing the single whole representations of secure endorsed transactions in the memory means.

5. In a network comprised of point of sale (POS) equipment distributed remotely from a central controller, wherein the POS equipment includes a transaction input device and an identifier input device, a process for generating secure endorsed transactions comprising the steps, performed by the POS equipment, of:

receiving transaction input and unique human identifiers;

generating unique codes from the transaction data and unique human identifiers, wherein the unique codes constitute secure endorsements of the transaction data by the individuals corresponding to the unique human identifiers; and

transmitting the unique codes along with the transaction input and unique human identifiers to the central controller, wherein the unique codes, the transaction input, and the unique human identifiers constitute secure endorsed transactions.

6. The process of claim 5, wherein the central controller is connectable by a telecommunications network to the POS equipment, and wherein the transmitting step further includes the substep of:

linking the POS equipment to the telecommunications network.

7. The process of claim 6, wherein the central controller receives a signal indicating that the POS equipment has linked to the telecommunications network and wherein the linking substep further includes the sub-substep of:

sending the unique codes along with the transaction input and unique human identifiers to the central controller via the telecommunications network.

8. The process of claim 5, wherein the transmitting step includes the substep of:

formatting the unique codes, the transaction data, and the unique human identifiers to produce single whole representations of secure endorsed transactions.

9. The process of claim 8, wherein the central controller is connectable by a telecommunications network to the POS equipment, and wherein the transmitting step further includes the substep of:

linking the POS equipment to the telecommunications network.

10. The process of claim 9, wherein the central controller receives a signal indicating that the POS equipment has linked to the telecommunications network and wherein the linking substep further includes the sub-substep of:

sending the single whole representations of secure endorsed transactions to the central controller via the telecommunications network.

11. A method of generating forge-resistant, tamper-resistant secure endorsed transactions comprised of transaction data representative of transactions, unique human identifiers corresponding to at least one party, called first party, endorsing a transactions, and public keys corresponding to at least a second party endorsing a transaction, wherein the public keys have corresponding private keys maintained in secret by the second party, the method comprising the steps, performed by a data processing system, of:

receiving transaction data, a unique human identifier, and a public key;

generating a unique code from the transaction data, the unique human identifier, and the public key, wherein the unique code constitutes a secure endorsement of the transaction data by the first party; and

generating, using a private key corresponding to the received public key, a digital signature of the unique code, wherein the digital signature constitutes a secure endorsement of the transaction data by the second party.

12. The method of claim 11 wherein the second generating step includes the substep of:

formatting the digital signature, the transaction data, the unique human identifier, and public key to produce a single whole representation of the tamper-resistant secure endorsed transaction.

13. The method of claim 11, wherein the data processing system includes a storage means, and wherein the second generating step includes the substep of:

storing the digital signature, the transaction data, the unique human identifier, and the public key in the memory means.

14. The method of claim 12, wherein the data processing system includes a storage means, and wherein the formatting step includes the substep of:

storing the single whole representations of tamper-resistant secure endorsed transaction in the memory means.

15. A method of verifying secure endorsed transactions comprised of transaction data representative of transactions, unique human identifiers corresponding to individuals endorsing the transactions, and unique codes generated from the transaction data and unique human identifiers, method comprising the steps, performed by a data processing system, of:

receiving secure endorsed transactions; and

generating unique codes from the transaction data and unique human identifiers of the secure endorsed transactions, wherein the unique codes constitute secure endorsements of the transaction data by the individuals corresponding to the unique human identifiers; and

comparing the unique codes of the received secure endorsed transactions with the generated unique codes to determine if there is a match, wherein if the unique codes of the received secure endorsed transactions match the generated unique codes then neither the transaction data nor unique human identifiers of the secure endorsed transactions have been altered prior to execution of the verification method.

16. In a network comprised of point of sale (POS) equipment distributed remotely from a central controller, wherein the POS equipment includes a transaction input device and an identifier input device, a process for verifying secure endorsed transactions having transaction data representative of transactions, unique identifiers corresponding to parties endorsing the transactions, and unique codes generated from the transaction data and unique identifiers, comprising the steps, performed by the POS equipment, of:

receiving secure endorsed transactions;

generating unique codes from the transaction data and unique identifiers of the secure endorsed transactions, wherein the unique codes constitute secure endorsements of the transaction data by the parties corresponding to the unique identifiers; and

comparing the unique codes of the received secure endorsed transactions with the generated unique codes to determine if they match, wherein if the unique codes of the received secure endorsed transactions match the generated unique codes then neither the transaction data nor unique identifiers of the secure endorsed transactions have been altered prior to execution of the verification process.

17. The process of claim 16, wherein the comparing step includes the substep of:

transmitting verification signals to the central controller indicating that neither the transaction data nor the unique identifiers of the secure endorsed transactions have been altered prior to execution of the verification process.

18. The process of claim 16, wherein the POS equipment includes an output display, and wherein the comparing step includes the substep of:

displaying verification messages indicating that neither the transaction data nor unique identifiers of the secure endorsed transactions have been altered prior to execution of the verification process.

19. A method of verifying a tamper-resistant secure endorsed transactions comprised of transaction data representative of a transaction, a unique identifier corresponding to at least one party, called a first party, endorsing the transaction, a public key corresponding to at least a second party endorsing the transaction, wherein the public key has a corresponding private key maintained in secret by the second party, and a digital signature generated using the private key corresponding to the public key, wherein the digital signature constitutes an endorsement by the second party of the transaction, the method comprising the steps, performed by a data processing system, of:

receiving a tamper-resistant secure endorsed transaction;

generating a stored unique code from the digital signature and the public key of the tamper-resistant secure endorsed transaction;

generating a unique code from the public key, the human identifier, and the transaction data of the tamper-resistant secure endorsed transaction; and

comparing the unique code with the stored unique code to determine if they match, wherein if the stored unique code matches the generated unique code then neither the transaction data nor unique identifiers of the tamper-resistant secure endorsed transaction was altered prior to execution of the verification process.

20. The process of claim 5, wherein the POS equipment includes a smart card device for reading/writing card data for the transaction data from smart cards, wherein the receiving step includes the substeps of:

receiving signals from the smart card device indicating the insertion of smart cards; and

acquiring card data from the inserted smart cards for inclusion in the transaction data.

21. The process of claim 20, wherein the transmitting step includes the substep of: dispatching the secure endorsed transactions to the inserted smart cards.

22. The process of claim 20, wherein the transmitting step includes the substep of: writing the secure endorsed transactions on the inserted smart cards.

23. In a network comprised of point of sale (POS) equipment distributed remotely from a central controller, wherein the POS equipment includes a transaction input device for receiving transaction input and an identifier input device for receiving unique identifiers optionally connectable to a smart card device for reading/writing card data from smart cards and writing data representative of secure endorsed transactions to smart cards, a process for generating secure endorsed transactions comprising the steps, performed by the POS equipment, of:

receiving a signal indicating insertion of a smart card in the smart card device;

reading card data from the inserted smart card;

receiving transaction input from the transaction input device;

combining the card data and transaction input to form a transaction data representative of a complete transaction;

receiving a human identifier from the identifier input device, the unique identifier corresponding to a party endorsing the complete transaction;

generating a unique code from the transaction data and the unique identifier, wherein the unique code constitutes an endorsement of the complete transaction by the party corresponding to the unique identifier; and

storing the unique code along with the transaction data and unique identifier on the smart card, wherein the unique code, the transaction data, and the unique identifier combined constitute a secure endorsed transaction.

25. The process of claim 1, wherein the data processing system includes a smart card device for reading/writing card data for the transaction data from smart cards wherein the receiving step includes the substeps of:

receiving signals from the smart card device indicating the insertion of a smart card; and

acquiring card data from the inserted smart card for inclusion in the transaction data.

26. The process of claim 25, wherein the transmitting step includes substep of:

dispatching the secure endorsed transaction to the inserted smart card.

27. The process of claim 26, wherein the transmitting step includes the substep of:

writing the secure endorsed transaction on the inserted smart card.

29. The process of claim 11, wherein the data processing system includes a smart card device for reading/writing card data for the transaction data from smart cards wherein the receiving step includes the substeps of:

receiving signals from the smart card device indicating the insertion of a smart card; and

acquiring card data from the inserted smart card for inclusion in the transaction data.

30. The process of claim 29, wherein the transmitting step includes substep of: dispatching the secure endorsed transaction to the inserted smart card.

31. The process of claim 30, wherein the transmitting step includes the substep of: writing the secure endorsed transaction on the inserted smart card.